REMARKS

Applicants have thoroughly considered the Examiner's remarks in the September 15, 2008 Office action and have amended the application to more clearly set forth aspects of the invention. Claims 1-3, 5-24, and 26-40 are presented in the application for further examination. Claims 1, 2, 14, 16, 17, 20, 26, 27, 33, 34, and 40 have been amended by this Amendment C. Reconsideration of the application claims as amended and in view of the following remarks is respectfully requested.

Claim Rejections under 35 U.S.C. § 102

Claims 1–3, 5–10, 15–19, 21, 22, 26–30, and 32–38 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Pub. No. 2004/0255155 A1 (hereinafter "Stading"). Applicants respectfully disagree and submit that Stading fails to disclose each and every element of the claims.

Claims 1–3, 5–10, and 15

Amended independent claim 1 recites a method of detecting an attack on an authentication service, with the method comprising, among other things:

> storing data relating to a plurality of authentication requests communicated to an authentication service from a plurality of user agents via a data communication network, said requests each including a login identifier, a network address from which the request was communicated, and a password, and wherein storing the data relating to the requests comprises storing the login identifier and network address and storing the password of each of the requests in a database of the authentication service only if the request is unsuccessful;
>
> searching the stored data based on a query variable to identify a plurality of the requests communicated from at least one of the plurality of the user agents,
>
> comparing the stored data associated with the identified requests with a predefined pattern characterizing an attack based on the stored data of the identified requests to determine when the identified requests indicate the characterized attack on the authentication service; and
>
> detecting the attack in response to determining that the identified requests indicate the characterized attack.

In order to detect an attack, the method of claim 1 stores data relating to authentication requests communicated to an authenticated service from one or more user agents via a data

communication network. For example, Fig. 1 of the present Specification provides an exemplary illustration of a data communication network in which embodiments of the present invention may be utilized. Client computer systems (102) and affiliate servers (106) (alternately referred to as "web servers" or "network servers") are connected to a data communication network (104). (Specification, [0027]). The affiliate servers of this example use an authentication service provided on an authentication server (108) to validate a user when the user on a client computer system attempts to access an affiliate server. (Specification, [0026]). The attack detection method of claim 1 stores the authentication request data in a database. The stored data is then searched based on a query variable and compared to pre-defined attack characterization patterns to assess if one or more attacks have occurred. (Specification, [0040]). Table 1 and paragraphs [0042]-[0053] describe exemplary comparison patterns that may be used to determine if an attack has occurred. As an example, "Attack Type B" describes a non-distributed account-harvesting attack pattern, characterized by a single network address, multiple user accounts, and a single password. In other words, "a single network address uses the same password to try to sign in multiple user accounts." (Specification, Table 1 and [0044]). On the basis of predefined patterns, an operator or automated process can detect multiple types of attacks on an authentication service, including but not limited to, "brute force attacks, account-harvesting attacks, distributed attacks, and DoS [denial of service] attacks", which can then be remedied in an appropriate fashion such as, but not limited to, blocking the network address or addresses communicating the requests. (Specification, [0007]).

Applicants submit that the cited reference fails to show all of the elements of amended independent claim 1. According to the Examiner, Stading discloses a method of detecting an attack on an authentication service, with the method disclosing each element of claim 1. However, Stading does not disclose each and every element of amended independent claim 1. Stading describes its invention as:

> Detecting attacks on secured computer resources, including gathering user security data for a user having a user password protecting resources on a computer system; generating an alert password that is easier to crack than the user password; and deploying the alert password on the computer system for use in detecting password attacks on the protected resources. Generating an alert password that is easier to crack than the user password in some embodiment further

> comprises: generating an alert password having a cracking difficulty; attempting to crack the alert password and the user password until one cracks; and if the user password cracks first, repeatedly carrying out the following steps so long as the user password continues to crack first: generating an alert password having a reduced cracking difficulty; and attempting to crack both the alert password having a reduced cracking difficulty and the user password until one cracks.

(Stading, Abstract). Stading further describes its area of concern as follows:

> **[0035]** The password cracking attacks of concern are of the kind sometimes called 'dictionary attacks' or 'password guessing attacks.' That is, dictionaries are used by cracking programs as input data for password guessing algorithms. Passwords guessed by the cracking programs are then used in attacking computer security systems. This approach, unfortunately, is very successful. It only takes one success to break into a secured computer system. Cracking programs using small dictionaries have been shown to be successful as much as 20% of the time. Large dictionaries can contain many megabytes of words and word stems from most written languages. Dictionaries can contain all the kinds of user security data described just above and more, names, addresses, numbers, hobbies, favorite authors, and so on.

In addressing this area of concern, Stading discloses the generation and assignment of "alert passwords". (Stading, [0032] and [0036]). In order to prevent dictionary-type password attacks, each user is assigned a decoy "alert password" that is generally easier to guess than the user's actual password – if a submitted password matches a user's alert password, the system concludes that the user account is under attack. (Stading, [0038]). The Stading invention then responds to protect the attacked user account by notifying system administrators of the attack on the account, limiting resources that the user account can access, suspending/terminating all permissions on the user account, and attempting to trace the attack and identify the attacker. (Stading, [0038]). In other words, the attack detection and response in Stading is a **user account-centric** mechanism, with attacks are signaled on the basis of the submission of the user account's alert password and corrective actions are taken on the user account level.

However, the method of amended claim 1 recites, among other things, storing data relating to a plurality of authentication requests communicated to an authentication service from a plurality of user agents, "wherein **storing the data relating to the requests** comprises storing the login identifier and network address and storing the password of each of the requests in a

database of the authentication service only if the request is unsuccessful", and then "comparing the stored data associated with the **identified requests** with a **predefined pattern characterizing an attack based on the stored data** of the identified requests to determine when the identified requests indicate the characterized attack on the authentication service." The method of claim 1 detects authentication service attacks by analyzing and comparing the stored data of a plurality of authentication requests to **predefined attack characterization patterns**. Detection of an attack occurs when the stored data of the requests matches one or more of the predefined patterns. Stading does not disclose or teach a method of attack detection on the basis of authentication request patterns - in fact, Stading teaches away from a pattern-based method, since its detection mechanism determines an attack on a user account has occurred when a submitted password matches the "alert password". Stading does not disclose storing data relating to a plurality of authentication requests for use in attack detection, but instead relies upon the single "alert password" match to determine an attack has occurred. Unlike the method of claim 1, Stading cannot detect patterns such as brute force attacks, account-harvesting attacks ("Attack Type B" pattern as described above), distributed attacks, or DoS attacks, as Stading cannot recognize attack patterns in data it does not have. Stading discloses neither storing authentication request data nor comparing the stored data with predefined attack characterization patterns, and therefore fails to disclose each and every element of the method of amended independent claim 1.

In view of the foregoing, Applicants submit that amended independent claim 1 and its dependent claims 2, 3, 5–10, and 15 are patentable for at least the reasons given above and rejection under 35 U.S.C. § 102(e) should be withdrawn.

Claims 16–19, 21, and 22

With respect to the subject matter of amended independent claim 16 and its dependent claims 17–19, 21, and 22, the Examiner rejects 16–19, 21, and 22 for the same essential reasons given for the rejection of claims 1–3, 5–10, and 15. Applicants respectfully disagree and submit that claims 16–19, 21, and 22 are allowable for at least the same reasons given above for the allowance of claims 1–3, 5–10, and 15. As such, rejection of amended independent claim 16 and its dependent claims 17–19, 21, and 22 under 35 U.S.C. § 102(e) should be withdrawn.

Claims 26–30 and 32

With respect to the subject matter of amended independent claim 26 and its dependent claims 27–30 and 32, the Examiner rejects 26–30 and 32 for the same essential reasons given for the rejection of claims 1–3, 5–10, and 15. Applicants respectfully disagree and submit that claims 26–30 and 32 are allowable for at least the same reasons given above for the allowance of claims 1–3, 5–10, and 15. As such, rejection of amended independent claim 26 and its dependent claims 27–30 and 32 under 35 U.S.C. § 102(e) should be withdrawn.

Claims 33–38

With respect to the subject matter of claims 33–38, the Examiner rejects 33–38 for the same essential reasons given for the rejection of claims 1–3, 5–10, and 15. Applicants respectfully disagree and submit that claims 33–38 are allowable for at least the same reasons given above for the allowance of claims 1–3, 5–10, and 15. As such, rejection of amended independent claim 33 and its dependent claims 34–38 under 35 U.S.C. § 102(e) should be withdrawn.

Claim Rejections under 35 U.S.C. § 103

Claims 11, 12, 23, 24, 31, and 39

Claims 11, 12, 23, 24, 31, and 39 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Stading in view of U.S. Pub. No. 2002/0097145 (hereinafter "Tumey"). Applicants respectfully disagree, as none of the cited references, alone or in combination, disclose each and every element of dependent claims 11, 12, 23, 24, 31, and 39.

Tumey fails to cure the deficiencies of Stading noted above. Tumey states:

> **[0008]** In accordance with the foregoing objects, the present invention—a method and apparatus for preventing theft of, and/or facilitating authorized access to, automotive vehicles—generally comprises an image acquisition device adapted to generate signals representative of a human facial image wherein a processor associated with the image acquisition device is adapted to operatively receive the signals and generate an output relative to recognition or non-recognition of the human facial image. A response interface

> is associated with the processor and adapted to effect a vehicle security measure responsive to the recognition or non-recognition of the human facial image. The system may also comprise an enrollment interface adapted for enrolling authorized human users.

The Tumey invention, like Stading, is a **user-centric** mechanism, where an intrusion is signaled by a single instance of non-recognition of a human facial image, and not upon a detected pattern. Additionally, Applicants respectfully disagree that Tumey is an analogous art to either Stading or the present invention. As shown above in Tumey, paragraph [0008], Tumey is directed towards a facial recognition vehicle security system. It would not have been obvious to one skilled in the arts of Stading or the present invention to incorporate disclosures or suggestions from a facial recognition vehicle security system when designing methods and systems for detecting patterns of attack against a user authentication service on a data network. Applicants respectfully request a reference citation from the Examiner disclosing or suggesting this combination. However, even in combination, Stading and Tumey fail to disclose **pattern-based attack detection**.

Applicants submit that dependent claims 11, 12, 23, 24, 31, and 39 are allowable for at least the same reasons stated above for the allowance of the independent claims from which claims 11, 12, 23, 24, 31, and 39 respectively depend. As such, rejection of dependent claims 11, 12, 23, 24, 31, and 39 under 35 U.S.C. § 103(a) should be withdrawn.

Claims 13, 14, 20, and 40

Claims 13, 14, 20, and 40 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Stading in view of U.S. Pub. No. 2003/0145225 (hereinafter "Bruton"). Applicants respectfully disagree, as none of the cited references, alone or in combination, disclose each and every element of dependent claims 13, 14, 20, and 40.

A combination of Stading and Bruton also fails to recite all the elements of dependent claim 13, 14, 20, and 40 and the independent claims upon which they depend. As noted above, Stading does not disclose methods or systems that store data relating to a plurality of **authentication requests** communicated to an authentication service from a plurality of user agents via a data communication network as indicated in amended independent claims 1, 16, and 33. Stading is a user-centric mechanism that relies on a single decoy "alert password" match to indicate an attack. Bruton fails to cure this deficiency, as the mechanism in Bruton relies on

network packet inspection to test for suspect data packets, e.g. malformed data packets. (*See* Bruton, [0050] and [0074]). In this manner, a plurality of authentication requests comprised of well-formed data packets would not signal an intrusion in Bruton, while the methods and systems of claims 1, 16, and 33 would examine the authentication requests for predefined attack patterns and detect authentication service attacks that Bruton could not.

Applicants submit that dependent claims 13, 14, 20, and 40 are allowable for at least the same reasons stated above for the allowance of the independent claims from which claims 13, 14, 20, and 40 respectively depend. As such, rejection of dependent claims 13, 14, 20, and 40 under 35 U.S.C. § 103(a) should be withdrawn.

Conclusion

Applicants submit that the claims are allowable for at least the reasons set forth herein. It is felt that a full and complete response has been made to the Office action and, as such, places the application in condition for allowance. Such allowance is hereby respectfully requested.

Although the prior art made of record and not relied upon may be considered pertinent to the disclosure, none of these references anticipates or makes obvious the recited aspects of the invention. The fact that Applicants may not have specifically traversed any particular assertion by the Office should not be construed as indicating Applicants' agreement therewith.

Applicants wish to expedite prosecution of this application. If the Examiner deems the application to not be in condition for allowance, the Examiner is invited and encouraged to telephone the undersigned to discuss making an Examiner's amendment to place the application in condition for allowance.

The Commissioner is hereby authorized to charge any deficiency or overpayment of any required fee during the entire pendency of this application to Deposit Account No. 19-1345.

Respectfully submitted,

/Robert M. Bain/

Robert M. Bain , Reg. No. 36,736
SENNIGER POWERS LLP
100 North Broadway, 17th Floor
St. Louis, Missouri 63102
(314) 231-5400

RMB/ALB/axj